

ERNEST J. ISTOOK, JR.
5TH DISTRICT, OKLAHOMA

COMMITTEE:
APPROPRIATIONS
SUBCOMMITTEES:
CHAIRMAN,
DISTRICT OF COLUMBIA
LABOR, HHS, AND EDUCATION
DEFENSE
ASSISTANT MAJORITY WHIP

Congress of the United States
House of Representatives
Washington, DC 20515-3605

February 22, 2001

DOCKET FILE COPY ORIGINAL

2404 RAYBURN BUILDING
WASHINGTON, DC 20515-3605
(202) 225-2132
FAX (202) 226-1463

DISTRICT OFFICES:
5400 N. GRAND BOULEVARD
SUITE 505
OKLAHOMA CITY, OK 73112
(405) 942-3636
FAX (405) 942-3792

117 W. 5TH STREET
BARTLESVILLE, OK 74603
(918) 336-5546
FAX (918) 336-5740

5TH & GRAND
PONCA CITY, OK 74601
(580) 762-6778
FAX (580) 762-7049
istook@mail.house.gov

Magalie Roman Salas
Office of the Secretary
Federal Communications Commission
445 12th St SW
Washington, D.C. 20554

Sheryl Todd
Accounting Policy Division
Common Carrier Bureau
Federal Communications Commission
445 Twelfth St SW, Room 5-B540
Washington, D.C. 20554

RECEIVED
MAR - 5 2001
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

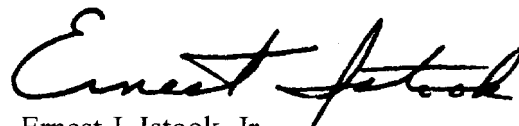
Subject: Reply Comments to Public Comment on CC Docket No. 96-45, The Children's
Internet Protection Act (CHIP)

Dear Madam Secretary:

As a major author of the Children's Internet Protection Act, I am providing
a reply comment on the notice of proposed rulemaking, CC Docket No. 96-45. My reply
is attached.

If you have questions, please feel free to call me or my staff member, Dr. Bill
Duncan, at (202) 225-2132.

Very truly yours,



Ernest J. Istook, Jr.
Member of Congress

EJI/wad

No. of Copies rec'd 0
List A B C D E

REPLY COMMENTS

RECEIVED

MAR - 5 2001

**FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY**

OF

**ERNEST J. ISTOOK, JR.
MEMBER OF CONGRESS
THE FIFTH DISTRICT OF OKLAHOMA**

REGARDING NOTICE OF PROPOSED RULE MAKING

IMPLEMENTING

THE CHILDREN'S INTERNET PROTECTION ACT

CC DOCKET NUMBER 96-45

FEBRUARY 22, 2001

**Submitted by:
Representative Ernest J. Istook, Jr.
Member of Congress
Contact:: Dr. Bill Duncan
(202)225-2132**

After reviewing public comments on the notice of proposed rule making to implement the Children's Internet Protection Act (the Act), as one of the principal authors of the Act, I submit the following reply comments:

I. Timing of Certification in Funding Year Four

Some commentors suggest that the Act should not apply until July 1, 2002, the start of year five of the schools and libraries universal services funding mechanism. However, as the FCC correctly noted in its notice of proposed rule making, the Act is quite explicit - the Act applies to the first program funding year following the December 21, 2000 effective date. That is funding year four, which begins on July 1, 2001.

Suggestions that funding years do not start on July 1, but instead begin "in theory" (as one commentator put it) with the filing of application forms the previous November stretches credulity. Moving the application of the Act to funding year five would be in direct conflict with the law and is beyond the scope of the agency's authority.

A variety of supposedly perceived problems associated with implementation in year four are raised by several school and library commentators as reasons for suggesting that implementation should begin in year five. However, the Act already provides a mechanism for overcoming all such problems, namely that in the initial year entities need not certify that they are in compliance. Instead, they may certify that they are "putting in place" Internet safety policies and technological protection measures. True compliance need not be certified until the following year.

If the FCC were to cite year five as the initial year of implementation, that would mean that true compliance need not occur until year six, in 2003. There is no justifiable reason for waiting that long--nor is there authority to ignore Congress' clear instructions otherwise.

II. Proposed Exceptions to the Act

Similarly, the FCC has no authority to create exceptions to the Act, as some have commentors suggested. Exceptions are proposed, for example, for computers not available for public use. It is beyond the scope of the FCC's authority to make exceptions to Congress' instructions covering computers with access to the Internet (as defined in my previous letter).

The Act specifically refers to certification by schools and libraries with respect to "any of its computers with Internet access" (emphasis added) and does not contain language limiting coverage to computers used by the public. As I mention in my previous letter, if the Internet is used as a pipeline to a closed system without world wide web access available, and no prohibited material is available in that closed system,

that is one thing. But to exempt computers purchased with Federal funds or granted access with e-rate funds, even though they have web access (http, ftp, etc.), is not within the FCC's discretion under the legislation.

III. Exemption from Liability by School and Library Districts or other Consortia

Some commentators have asked the FCC to create an exemption from liability if school and library districts or other consortia certify that individual schools or libraries within their systems are in compliance when, in fact, they are not. This is an incredible request! Not only should no such exemption be granted, but the FCC must insist on enforcing the Congressionally-mandated liability.

If certification is made by districts or consortia on behalf of their individual institutions, those certifying bear the responsibility of verifying whether the requirements of the Act have indeed been met by individual institutions under their control. They cannot substitute subterfuge for compliance. Liability ensures accountability.

The concern over liability is easily handled by giving districts and consortia a choice. The FCC should allow them to certify themselves AND assume liability, or direct each school and library within their system or consortia to certify on their own.

IV. A Definitive Public Hearing Requirement

Language in the Act links the hearing requirement to "the proposed" Internet safety policy. Some commentators suggest that this means a public hearing is not required if there is already a policy in place. A close reading of the Act, however, indicates that a hearing is required in all cases. The language, "the proposed", refers back to an earlier section describing the *new* policy required under the Act, not to policies already in place (which may or may not restrict access to the specific content categories enumerated in the Act). The intent of the legislation clearly is to require new public hearings regarding this Internet Safety policy. This is to satisfy definitions of obscenity under existing Supreme Court case law, which requires that there be local input into that standard. This hearing also allows action on anything else the community believes should be included in protection for minor, such as bomb-making.

V. Quantifying Effectiveness and Need

In my previous comments, I urged the FCC to require schools and libraries to establish a public comment procedure and to keep a written log of complaints and comments received. I reiterate this suggestion and also associate myself with a suggestion in comments made by the National Law Center for Children and Families,

which further improves upon my comments. After the first year of compliance, certification should include key statistics, including the number of:

- website visits,
- attempts to access sites whose content is restricted under the Act,
- instances in which such content was not blocked, as reported in complaints,
- instances in which unrestricted content was blocked, as reported in complaints, and,
- instances in which disabling occurred for "bona fide research or other lawful purposes," as is allowed under the Act.

Technology protection measures can readily track the first two items without identifying the user, which is prohibited under the Act. The other items can be tracked through school and library public comment logs. Such data should be reported to the FCC as part of compliance and should be publicly posted at each school and library. Easy public access to such information will go a long way toward dispelling myths and misperceptions about the safety of schools and libraries and the effectiveness of technology protection measures.